IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	David J. Wetherall *et al.*	Confirmation No:	8089
Application No:	09/706,503	Group:	2142
Filed:	November 2, 2000	Examiner:	Biagini, Christopher D.
For:	Detecting and Preventing Undesirable Network Traffic from Being Sourced out of a Network Domain		
Customer No.:	29127		

Attorney Docket No.	0016.0005US

Revised APPELLANT'S BRIEF

Commissioner for Patents
P.O. Box 1450,
Alexandria, Virginia 22313-1450

Sir:

This is the Applicants' appeal from the final Office Action, mailed February 28, 2008 (Paper No. 20080222). This is further in response to a Notification of Non-Compliant Appeal Brief mailed November 19, 2008.

A two-month extension of time was requested for this response.

Real Party in Interest

Arbor Networks, Inc. is the real party in interest.

Related Appeals and Interferences

There are no related appeals or interferences.

Status of Claims

Claims 1, 3, 5-14, 16, 18-27, 29, 31-39, 42-48 and 51-58 are pending in this application. Claims 2, 4, 15, 17, 28, 30, 40, 41, 49 and 50 are cancelled. Claims 1, 3, 5-14, 16, 18-27, 29, 31-39, 42-48 and 51-58 are rejected and hereby appealed.

Status of Amendments

All amendments have been entered. There were no post final amendments or proposed amendments.

Summary of Claimed Subject Matter

Claim 1 concerns a network comprising:

a first network domain which is a local area network (see specification at page 7, line 7, and Fig. 3A, reference numeral 104');

a first routing device at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric (see specification at page 7, line 13, and Fig. 3A, reference numeral 114'); and

a monitor/regulator, either integrally disposed in said first routing device or coupled to the first routing device to monitor the network traffic routed by said first routing device by analyzing flow records, describing traffic conversation as indicated by a combination of source and destination addresses, received from the routing device, the monitor/regulator determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain (see specification at page 7, line 9, and Fig. 3A, reference numeral 102'),

wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said first network domain

relative to network traffic routed into said first network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain (see specification at page 9, lines 24-26).

Claim 14 concerns a network traffic regulation method comprising:

monitoring network traffic routed by a first routing device of a first network domain which is a local area network (see specification at page 6, line 11, and Fig. 2, reference numeral 202); and

determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against to a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain, wherein the first network domain is determined to be sourcing undesirable network traffic by analysis of flow records describing traffic conversation, as indicated by a combination of source and destination addresses, received from the first routing device, which is positioned at a boundary between the local area network and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric (see specification at page 6, line 13, and Fig. 2, reference numeral 204);

wherein said determining comprises determining based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into the network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain (see specification at page 9, lines 24-26).

Claim 27 concerns an apparatus comprising:

(a) storage medium having stored therein a plurality of programming instructions designed to enable the apparatus to monitor network traffic routed by a first routing device of a first network domain which is a local area network, the first routing device in the local area network at a boundary between the local area network and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric; and programming instructions designed to enable the apparatus to analyze flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device and determine if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against to a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain (see specification at page 18, lines 18- 26, and Fig. 4, reference numeral 414a, 414b, page 7, line 9, and Fig. 3A, reference numeral 102'); and

(b) a processor coupled the storage medium to execute the programming instructions (see specification at page 18, lines 111, and Fig. 4, reference numeral 402);

wherein the programming instructions enable the apparatus to make said determination based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into the network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain (see specification at page 9, lines 24-26).

Claim 58 concerns a network comprising:

a network domain which is a local area network (see specification at page 7, line 7, and Fig. 3A, reference numeral 104');

a routing device in the local area network at a boundary between the local area network and public internetworking fabric to route network traffic between the network domain and the public internetworking fabric (see specification at page 7, line 13, and Fig. 3A, reference numeral 114'); and

a monitor/regulator, either integrally disposed in said routing device or coupled to the routing device, to monitor the network traffic routed by said routing device by analyzing flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device, the monitor/regulator determining if the network domain is sourcing undesirable network traffic that is originating in the network domain and being routed out of the network domain by the routing device, the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable network traffic, wherein said monitor/regulator instructs the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic (see specification at page 7, line 9, and Fig. 3A, reference numeral 102');

wherein the undesirable network traffic comprises a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the network domain (see specification at page 21, beginning at line 21);

wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into said network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain (see specification at page 9, lines 24-26).

Grounds of Rejection to be Reviewed on Appeal

Whether claims 1, 3, 5-14, 16, 18-27, 29, 31-39, 42-48 and 51-58 are unpatentable under 35 U.S.C. 103(a) over Malan *et al.* (US PGPUB 2002/0032871, hereinafter "Malan") in view of Poletto *et al.* (US PGPUB 2002/0032880, hereinafter "Poletto").

Argument

Pending Claims are Patentable over Malan in view of Poletto

Scope and Content of Applied Art

Denial of service (DoS) attacks are a type of cyber attack in which the attacker seeks to overload the target website or other web service. Today, a common approach to mitigating DoS attacks is to configure networking devices, such as routers, to block or drop packets from the attacker or computers that have been co-opted by the attacker (zombies). For example, a router that sends packets to and receives packets from a targeted server is configured to drop packets from certain internet protocol (IP) addresses originating the DoS packets.

Simply blocking the packets at the router that is upstream of the targeted server does not address all symptoms of the DoS attack. Such blocking can certainly allow the targeted server to continue to function. On the other hand, the DoS attack will continue to consume bandwidth on the network backbone to the upstream router.

Malan teaches that back-tracing can be used to block DoS packets closer to the source. For example, paragraph [0077] of Malan teaches a tracing technique:

> [0077] Once the controller has received the alert message from the collector **20**, the controller **24** can apply several approaches to trace the DoS attack back to its origin, such as, directed tracing or distributed correlation. In directed tracing, information related to the computer network system topology is processed to work backwards towards the source or origin of the DoS attack. Directed tracing relies on the fact that both the router system's incoming interface statistic for a DoS attack and information related to the computer network system **10** topology are known to determine what routers are upstream on a particular link that carried the DoS attack packet. With this knowledge, upstream routers (not shown) can then be queried for their participation in transiting the attack packet. It is useful to note that since these upstream routers are looking for a specific attack signature, it is much easier to find the statistics related to the attack packet.

Back-tracing and then configuring those routers to drop the DoS packets enables further mitigation in terms of preserving bandwidth through the network.

Poletto describes a distributed system for detecting DoS attacks. It uses gateways and data collectors to monitor traffic and look for indications of DoS attacks. For example, paragraph [0022] of Poletto provides:

> sible to the attacker. The gateway **26** devices are located at the edges of the Internet **14**, for instance, at the entry points of data centers. The gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a DoS attack. The data collectors **28** are located inter alia at major peering points and network points of presence (PoPs). The data collectors **28** sample packet traffic, accumulate, and collect statistical information about network flows.

Poletto teaches the use of a control center that receives messages from a gateway data collector that a victim is under attack. This is described at paragraph [0040] of Poletto:

> data collectors **28**. The gateway **26** at the victim **12** contacts the control center and notifies the control center **24** that the victim **12** data center is under a spoofing attack. The gateway **26** identifies itself by network address (e.g., static IP address if on the Internet **14**), via a message to the control center **24**. The message sent over the hardened network **30** indicates the type of attack, e.g., an attack from addresses that the victim **12** cannot stop because it is a spoofing type of attack. The control center queries data collectors **28** and asks which data collectors **28** are seeing suspicious traffic being sent to the victim **12**.

The control center can then back-trace the attack, possibly to the gateway that the attacker is behind. This is described in paragraph [0042] of Poletto, for example:

> **[0042]** In the present configuration, there are two possible sources of attack traffic: either the attacker is behind a gateway **26** or not. If the attacker is behind a gateway **26**, the control center issues a request to the appropriate gateway **26** to block the attacking traffic, e.g. by allowing the appropriate gateway **26** to discard traffic, e.g., packets that contain the victim **12** destination address. The gateway **26** stops that

Differences between Applied Art and Claimed Invention

Each of claims 1, 14, 27, and 58 requires the detection of the DoS attack at routing device that is at the boundary between a network domain and a public internetworking fabric. It uses differential characteristics between request packets routed out of said network domain to determine if the network domain is sourcing undesirable packets of the DoS attack.

As described above and in contradistinction, the prior art references teach the detection of the DoS attack at or near the target of the attack.

Non-obviousness of Claimed Invention

This distinction, detection at source (present invention), instead of detection at target (Malan, Poletto) enables the present invention to ensure that the network domain, typically operated by the owner of the routing device, is not the source of DoS attacks. In

this way, the owner is able to avoid liability for damage or bandwidth consumption on networks owned by others. In contrast, when using the systems of others, it is only possible to stop at attack at the source when routers or monitors near the attack detect it. In short, Malan and Poletto rely on detection at the target, which are typically in networks of other entities. In contrast, the present invention ensures that network owners can be "good citizens" by ensuring that their networks are not the source of an attack.

Moreover, the present invention requires detection of the attack via a specific method: differential characteristics between request packets routed out of the network domain and response packets routed into the network domain. While this technique for detecting DoS attacks is not new in itself, none of the applied references teaches that this technique should be applied at the boundary router to determine whether the network domain is sourcing DoS packets as claimed.

For these reasons, it is respectfully asserted that the applied references neither show nor suggest features of the claimed invention and these features provide for improved operation over the applied references.

Non-obviousness of Claims 6, 19, and 32

Claims 6, 19, and 32 further describe a second routing device for the network domain and determining of the domain is sourcing DoS packet by reference to information from both routing devices for the domain. Neither of the applied reference shows a similar topology, two routers for a single domain, combined with detecting the DoS attack based on information from the two routing devices.

Thus, these claims are additionally distinguishable.

Non-obviousness of Claims 44 and 53

Claims 44 and 53 further describe a determining whether the domain is sourcing DoS packets based on time to live values for the packets.

The pending Office Action concedes that this functionality is not taught by the applied references, but nonetheless argues that this claimed feature would have been obvious.

It is well settled that the Examiner bears the initial burden of establishing a prima facie case. In re Oetiker, 977 F.2d 1443, 1445 (Fed. Cir. 1992). To establish a prima facie case of obviousness, all the claim features must be taught by the prior art. In re Royka, 490 F.2d 981, 985 (CCPA 1974). If examination at the initial stage does not produce a prima facie case of unpatentability, then without more the applicant is entitled to a grant of the patent. Oetiker, 977 F.2d at 1445.

Here prima facie obviousness has not been established. Thus, the rejection of these claims should be withdrawn for these additional reasons.

Non-obviousness of Claims 46, 55, and 58

Claims 46, 55, and 58 describe the monitor/regulator instructing a routing device to lower a priority of the undesirable network traffic.

The pending Office Action provided two sources for this claimed functionality in the applied references on its page 6:

> 15. Regarding claim(s) 46-47, 55-56, Malan further teaches slowing or lowing priority of traffic(60/231,481 pp. 10-11 as scanned, pp. 12-13 as labeled- describing how StormBreaker slows attack traffic to zero; Malan par. 79 showing CAR limiters).

It appears that the most relevant portion is the following paragraph from page 13 of the 60/231,481 application:

> StormBreaker determines the appropriate filtering response. Specifically, StormBreaker uses knowledge about the topology and infrastructure components in a network to make the best filtering decision. In this example, StormBreaker applies a filtering rule to the attacker's router to remove the its traffic from the network

This paragraph merely describes removing the traffic, not lowering its priority as claimed.

Lowering priority has advantages over removal since the traffic is not necessarily dropped and thus lost. As a result, any legitimate traffic caught within the filtering specifications is maintained, while mitigating the attack nonetheless.

For these reasons, these claims are additionally distinguishable.

Non-obviousness of Claims 48 and 57

Claims 46, 55, and 58 describe monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lowering a threshold for concluding that undesirable network traffic are being sourced out of another one of said first and second network domains.

The pending Office Action provided two sources for this claimed functionality on its page 6:

16. Regarding claim(s) 48, 57, Malan further teaches priority levels as groups/categories, par. 68, 70.

These paragraphs of Malan describe how thresholds are changed in networks, apparently as the network changes and evolves and does not appear to suggest the specifics of the claimed invention: upon determining a DoS attack in one domain, lowering thresholds associated with attack determination for other domains.

This claimed feature derives from the notion that the existence of an attack in one place may indicate an attack in another place, which is often possible since DoS attacks are often coordinated from many domains.

Thus, this claimed feature provides additional benefits over the systems described in the applied references and should be deemed to further distinguish the claimed invention.

For the foregoing reasons, Applicants believe that the pending rejections should be withdrawn, and that the present application should be passed to issue. Should any questions arise, please contact the undersigned.

Respectfully submitted,

Houston Eliseeva LLP

By /grant houston/
J. Grant Houston
Registration No.: 35,900
4 Militia Drive, Ste. 4
Lexington, MA 02421
Tel.: 781-863-9991
Fax: 781-863-9931

Date: December 12, 2008

Claims Appendix

1. (Previously presented) A network comprising:

a first network domain which is a local area network;

a first routing device at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric; and

a monitor/regulator, either integrally disposed in said first routing device or coupled to the first routing device to monitor the network traffic routed by said first routing device by analyzing flow records, describing traffic conversation as indicated by a combination of source and destination addresses, received from the routing device, the monitor/regulator determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain,

wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said first network domain relative to network traffic routed into said first network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

2. (Cancelled)

3. (Previously presented) The network of claim 1, wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

4. (Cancelled)

5. (Previously presented) The network of claim 1, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first domain, further stops said undesirable network traffic from being sourced out of said first domain.

6. (Original) The network of claim 1, wherein

said first network domain further comprises a second routing device for routing network traffic out of and into the first network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

7. (Original) The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

8. (Original) The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

9. (Original) The network of claim 6, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first network domain, further stops said undesirable network traffic from being sourced out of said first network domain.

10. (Original) The network of claim 1, wherein

said network further comprises a second network domain including a second routing device for routing network traffic out of and into the second network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if at least a selected one of the first and second network domains is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

11. (Original) The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

12. (Original) The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

13. (Original) The network of claim 10, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, further stops said undesirable network traffic from being sourced out of said first and second network domains.

14. (Previously presented) A network traffic regulation method comprising:

monitoring network traffic routed by a first routing device of a first network domain which is a local area network; and

determining if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against to a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain, wherein the first network domain is determined to be sourcing undesirable network traffic by analysis of flow records describing traffic conversation, as indicated by a combination of source and destination addresses, received from the first routing device, which is positioned at a boundary between the local area network and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric;

wherein said determining comprises determining based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into the network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

15. (Cancelled)

16. (Previously presented) The method of claim 14, wherein said determining comprises inferring said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

17. (Cancelled)

18. (Original) The method of claim 14, wherein the method further comprises stopping undesirable network traffics from being sourced out of said first network domain.

19. (Original) The method of claim 14, wherein the method further comprises

monitoring network traffic routed by a second routing device of said first network domain; and

determining if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

20. (Original) The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

21. (Original) The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

22. (Original) The method of claim 19, wherein the method further comprises stopping undesirable network traffic from being sourced out of the first network domain.

23. (Original) The method of claim 19, wherein the method further comprises

determining if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

24. (Original) The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic

characteristics observed of network traffic routed through said second as well as said first routing device.

25. (Original) The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

26. (Original) The method of claim 23, wherein the method further comprises stopping undesirable network traffic from being sourced out said first and/or second network domains.

27. (Previously presented) An apparatus comprising:

(a) storage medium having stored therein a plurality of programming instructions designed to enable the apparatus to monitor network traffic routed by a first routing device of a first network domain which is a local area network, the first routing device in the local area network at a boundary between the local area network and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric; and programming instructions designed to enable the apparatus to analyze flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device and determine if the first network domain is sourcing undesirable network traffic, comprising a denial of service attack in which the undesirable network traffic is launched against to a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the first network domain; and

(b) a processor coupled the storage medium to execute the programming instructions;

wherein the programming instructions enable the apparatus to make said determination based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into the network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

28. (Cancelled)

29. (Previously presented) The apparatus of claim 27, wherein the programming instructions enable the apparatus to infer said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

30. (Cancelled)

31. (Original) The apparatus of claim 27, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out of said first network domain.

32. (Original) The apparatus of claim 27, wherein the programming instructions enable the apparatus to monitor network traffic routed by a second routing device of said first network domain, and determine if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

33. (Original) The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

34. (Original) The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

35. (Original) The apparatus of claim 32, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said first network domain.

36. (Original) The apparatus of claim 27, wherein the programming instructions further enable the apparatus to determine if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

37. (Original) The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

38. (Original) The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

39. (Original) The apparatus of claim 36, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said first and/or second network domains.

40. (Cancelled)

41. (Cancelled)

42. (Previously presented) The network of claim 1, wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

43. (Previously presented) The network of claim 1, wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

44. (Previously presented) The network of claim 1, wherein said monitor/regulator generates statistics concerning distributions of time to live values and determines whether the first network domain is sourcing undesirable network traffic based on said statistics.

45. (Previously presented) The network of claim 1, wherein said monitor/regulator tracks differences between outbound transmission control protocol (TCP) synchronize (SYN) and finish (FIN) packets and inbound response packets and determines whether the first network domain is sourcing undesirable network traffic based on said differences

46. (Previously presented) The network of claim 1, wherein said monitor/regulator instructs a routing device to lower a priority of the undesirable network traffic.

47. (Previously presented) The network of claim 1, wherein said monitor/regulator instructs a routing device to slow the undesirable network traffic.

48. (Previously presented) The network of claim 10, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lower a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

49. (Cancelled)

50. (Cancelled)

51. (Previously presented) The method of claim 14, further comprising generating statistics concerning destination addresses and determining whether the first network domain is sourcing undesirable network traffic based on said statistics.

52. (Previously presented) The method of claim 14, further comprising generating statistics concerning lengths of packets and determining whether the first network domain is sourcing undesirable network traffic based on said statistics.

53. (Previously presented) The method of claim 14, further comprising generating statistics concerning distributions of time to live values and determining whether the first network domain is sourcing undesirable network traffic based on said statistics.

54. (Previously presented) The method of claim 14, further comprising tracking differences between outbound TCP SYN and FIN packets and inbound response packets and determining whether the first network domain is sourcing undesirable network traffic based on said differences

55. (Previously presented) The method of claim 14, further comprising instructing a routing device to lower a priority of the undesirable network traffic.

56. (Previously presented) The method of claim 14, further comprising instructing a routing device to slow the undesirable network traffic.

57. (Previously presented) The method of claim 23, further comprising, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, lowering a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

58. (Previously presented) A network comprising:

a network domain which is a local area network;

a routing device in the local area network at a boundary between the local area network and public internetworking fabric to route network traffic between the network domain and the public internetworking fabric; and

a monitor/regulator, either integrally disposed in said routing device or coupled to the routing device, to monitor the network traffic routed by said routing device by analyzing flow records describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device, the monitor/regulator determining if the network domain is sourcing undesirable network traffic that is originating in the network domain and being routed out of the network domain by the routing device, the monitor/regulator generating statistics concerning destination addresses to determine whether the network domain is sourcing the undesirable network traffic, wherein said monitor/regulator instructs the routing device to lower a priority of the undesirable network traffic and/or slow the undesirable network traffic;

wherein the undesirable network traffic comprises a denial of service attack in which the undesirable network traffic is launched against a target network device in order to undermine the operation of that target network device by overwhelming the target network device with network traffic, out of the network domain,

wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said network domain relative to network traffic routed into said network domain and aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

Evidence Appendix

None

Related Proceedings Appendix

None